UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/500,930	10/19/2005	Sami Vaarala	290.1078USN	1571

33369 7590 05/10/2011
FASTH LAW OFFICES (ROLF FASTH)
26 PINECREST PLAZA, SUITE 2
SOUTHERN PINES, NC 28387-4301

EXAMINER	
TOWFIGHI, AFSHAWN M	

ART UNIT	PAPER NUMBER
2469	

NOTIFICATION DATE	DELIVERY MODE
05/10/2011	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

sloan.smith@fasthlaw.com
nan_russell@fasthlaw.com

Office Action Summary	Application No.	Applicant(s)	
	10/500,930	VAARALA ET AL.	
	Examiner	Art Unit	
	AFSHAWN TOWFIGHI	2469	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *4/8/11*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-29 are pending.

2. Claims 28 and 29 are new.

Continued Examination Under 37 CFR 1.114

3. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 4/8/11 has been entered.

Response to Arguments

4. Applicant's arguments with respect to claims 1-29 have been considered but some are not persuasive and some are moot in view of the new ground(s) of rejection.

On page 4 of the applicant's response, the applicant states that the key in Kunzinger does not correspond to the unique identity of the present invention.

The examiner respectfully disagrees, but has provided clarification. The messages exchanged in Kunzinger are part of the IPSec protocol. The protocol uses messages that are encrypted and have a value associated them that is used by a key to read the

messages. Kunzinger [0067] shows that the messages have ID's associated them, in addition, IPSec uses a hash value that is transmitted with each packet. The "key" is the value that is transmitted with the packet so that it can be read by the receiving device. Therefore, as the claim language reads, the new combination of references does teach the argued limitations.

The examiner invites the applicant to contact the examiner to discuss the claim language and help further advance prosecution of the case.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1,2, 4-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kunzinger (Pub No: 2002/0091921)., and further in view of Gunter et al (Patent No: 7,055,027).

As to claim 1, Kunzinger teaches a method for secure forwarding of a message from a first computer to a second computer via an intermediate computer in a telecommunication network *(Kunzinger, [0047] L1-13, end to end data sending via an intermediate gateway using secure tunnels*), comprising:

in the first computer, forming a secure message by giving the secure message a first unique identity and a first destination address to the intermediate computer, *(Kunzinger, [0068] L1-3, the hash value of IPSec used by the key is the id and [0013] the outer header has the address of the endpoint of the tunnel, i.e. gateway),* sending the secure message containing the first unique identity and the first destination address from the first computer to the intermediate computer message *(Kunzinger, [0068] L1-3, the message is sent from the client and received by the gateway [0068] L1-3, the hash value of IPSec used by the key is the id and [0013] the outer header has the address of the endpoint of the tunnel, i.e. gateway),*

the intermediate computer receiving the secure message *(Kunzinger, [0068] L1-3, the message is sent from the client and received by the gateway)* and performing a translation by using the first unique identity to find a second destination address to the second computer *(Kunzinger [0074] the gateway uses tables and id to translate the packet into a corresponding tunnel and the data is then forwarded/send the over the second tunnel and [0013] the new packet has the address of the second computer),*

the intermediate computer substituting the first destination address with the second destination address to the second computer *(Kunzinger [0074] the gateway uses tables and id to translate the packet into a corresponding tunnel and the data is then forwarded/send the over the second tunnel and [0013] the new packet has the address of the second computer),*

the intermediate computer substituting the first unique identity with a second unique identity of the secure connection *(Kunzinger [0074] the gateway uses tables and id to translate the packet into a corresponding tunnel and the data is then forwarded/send the over the second tunnel and [0013] the new packet has the address of the second computer),* and the intermediate computer forwarding the secure message with the second destination address and the second unique identity to the second computer in the secure connection *(Kunzinger, [0074] forwarding the IPSec datagram and [0013] and [0068] the id and address are in the packet of data).*

Kunzinger does not expressly the first computer and the second computer negotiating and exchanging keys with one another according to a key exchange protocol to establish a secure connection between the first computer and the second computer via the intermediate computer, the secure connection having a source address of the first computer as a first end point and a destination address of the second computer as a second end point of the secure connection.

However, Gunter teaches the first computer and the second computer negotiating and exchanging keys with one another according to a key exchange protocol to establish a secure connection between the first computer and the second computer via the intermediate computer *(Gunter, Fig 4 and Col 6 L36-40, external client 42 and internal client 44 establish a secure connection via the intermediate firewall using a key exchange protocol)* the secure connection having a source address of the first computer as a first end point and a destination address of the second computer as

a second end point of the secure connection *(Gunter, Fig 4, the external client 42 is the source of the secure connection and the internal client 44 is the destination)*

It would have been obvious to one of ordinary skill in the art at the time of invention to combine the teachings of Kunzinger and Gunter to have the endpoints directly negotiate a key to establish a secure connection, because Gunter teaches that direct key negotiation is a well know method for two endpoints to communicate securely with an intermediary involved (Gunter Col 3 L50-57).

As to claim 2, Kunzinger and Gunter teaches wherein the method further comprises forming the secure message by using an IPSec connection between the first computer and the second computer *(Kunzinger, [0067], IPSec protection).*

As to claim 4, Kunzinger and Gunter teaches wherein the method further comprises manually performing a preceding distribution of keys to components for forming the IPSec connection *(Kunzinger, [0067], IKE is used to for the IPSec connection).*

As to claim 5, Kunzinger and Gunter teaches wherein the method further comprises performing a preceding distribution of keys for forming the IPSec connection by an automated key exchange protocol *(Kunzinger, [0067], IKE is used to for the IPSec connection).*

As to claim 6, Kunzinger and Gunter teaches wherein the method further comprises performing the automated key exchange protocol used for the preceding distribution of keys for forming the IP Sec connection by means of a modified IKE key exchange protocol between the first computer and the intermediate computer *(Kunzinger, [0067],*

using phase2 IKE exchange between the client and gateway, this is a modified protocol because the table at the gateway modifies the IKE packets and inserts a new address automatically) and by means of a standard IKE key exchange protocol between the intermediate computer and the second computer *(Kunzinger, [0069] using IKE between gateway and server).*

As to claim 7, Kunzinger and Gunter teaches wherein the method further comprises sending the message that is sent from the first computer as a packet that contains message data, an inner IP header containing the actual sender and receiver addresses, an outer IP header containing the addresses of the first computer and the intermediate computer, the unique identity *(Kunzinger, [0013], inner and outer headers and negotiated security association).*

As to claim 8, Kunzinger and Gunter teaches wherein the method further comprises the IPSec connection being one or more security associations (SA) and the unique identity being one or more SPI values*(Kunzinger, [0067], setting up the IPSec SA and the values are SPI values).*

As to claim 9, Kunzinger and Gunter teaches wherein the method further comprises performing the matching by using a translation table stored at the intermediate computer *(Kunzinger, [0066], the databases are the translation tables).*

As to claim 10, Kunzinger and Gunter teaches wherein the method further comprises changing both the address and the SPI-value by the intermediate computer *(Kunzinger,*

[0074], the address is changed to point to the tunnel and the ID(SPI) is changed, the SPI is the ID that is exchanged for indexing).

As to claim 11, Kunzinger and Gunter teaches wherein the method further comprises the first computer being a mobile terminal *(Kunzinger, [0038], the workstations communicate over a wireless cellular network)* so that the mobility is enabled by modifying the translation table at the intermediate computer *(Kunzinger, [0067] L13-17, the SAD on the gateway is modified with IKE value).*

As to claim 12, Kunzinger and Gunter teaches wherein the method further comprises performing the modification of the translation tables by sending a request for registration of the new address from the first computer to the intermediate computer *(Kunzinger, [0062], the client is the IKE initiator with negotiations with the gateway).*

As to claim 13, Kunzinger and Gunter teaches wherein the method further comprises sending a reply to the request for registration from the intermediate computer to the first computer *(Kunzinger, [0063], the gateway is the IKE responder to the client in the IKE negotiations).*

As to claim 14, Kunzinger and Gunter teaches wherein the method further comprises authenticating or encrypting by IPSec the request for registration and/or reply *(Kunzinger, [0067], authenticating IPSec).*

As to claim 15, Kunzinger and Gunter teaches wherein the method further comprises establishing the key distribution for the secure connections by establishing an IKE protocol translation table, and using the translation table to modify IP addresses and

cookie values of IKE packets in the intermediate computer *(Kunzinger [0074] the gateway uses tables and id to translate the packet into a corresponding tunnel and [0066]-[0067], the IKE protocol addresses, etc are stored in the SAD tables).*

As to claim 16, Kunzinger and Gunter teaches wherein the method further comprises establishing the key exchange distribution by: generating an initiator cookie and sending a zero responder cookie to the second computer, generating a responder cookie in the second computer *(Kunzinger, [0064] [0065] and [0067], the gateway is the initiator and the server is the responder in the IKE negotiations. [0069] shows an example of IKE negotiations the IDCi and IDCr values are set),* establishing a mapping between IP addresses and IKE cookie values in the intermediate computer, and using the translation table to modify IKE packets in flight by modifying the external IP addresses and possibly IKE cookies of the IKE packets *(Kunzinger [0074] the gateway uses tables and id to translate the packet into a corresponding tunnel and [0066]-[0067], the IKE protocol addresses, etc are stored in the SAD tables).*

As to claim 17, Kunzinger and Gunter teaches wherein the method further comprises modifying a modified IKE protocol between the first computer and the intermediate computer by transmitting the IKE keys from the first computer to the intermediate computer in order to decrypt and modify IKE packets *(Kunzinger, [0067], using phase2 IKE exchange between the client and gateway, this is a modified protocol because the table at the gateway modifies the IKE packets and inserts a new address automatically).*

As to claim 18, Kunzinger and Gunter teaches wherein the method further comprises carrying out in a modified IKE protocol between the first computer and the intermediate computer the modification of the IKE packets by the first computer with the intermediate computer requesting such modifications *(Kunzinger, [0067], using phase2 IKE exchange between the client and gateway, this is a modified protocol because the table at the gateway modifies the IKE packets and inserts a new address automatically).*

As to claim 19, Kunzinger and Gunter teaches wherein the method further comprises defining the address so that the first computer is identified for the second computer by the intermediate computer by means of an IP address taken from a pool of user IP addresses when forming the translation table *(Kunzinger [0074] the gateway uses tables and id to translate the packet into a corresponding tunnel and the data is then forwarded/send the over the second tunnel and [0013] the new packet has the address of the second computer).*

As to claim 20, Kunzinger and Gunter teaches wherein the method further comprises sending the secure message by using an IPSec transport mode *(Kunzinger, [0075] L12-15, IPSec operates in transport mode).*

As to claim 21, Kunzinger and Gunter teaches wherein the method further comprises sending the secure message by using an IPSec tunnel mode *(Kunzinger, [0075] L12-15, IPSec operates in tunnel mode).*

As to claim 22, Kunzinger teaches a telecommunication network for secure forwarding of messages *(Kunzinger, [0047] L1-13, end to end data sending via an intermediate gateway using secure tunnels),* comprising:

a first computer, a second computer and an intermediate computer *(Kunzinger, [0047] L1-13 and Fig 4, the endpoints and intermediate computer),*

the first and the second computers having means for performing an IPSec processing, the intermediate computer having translation means for using translation tables to perform IPSec and IKE translation and for changing a destination address of the intermediate computer of a secure message containing a unique identity to a destination address of the second computer *(Kunzinger [0074] the gateway uses tables and id to translate the packet into a corresponding tunnel (IKE/IPSec) and the data is then forwarded/send the over the second tunnel and [0013] the new packet has the address of the second computer),* and

the intermediate computer having means for using the unique identity when forwarding the secure message received from the first computer to the second computer in the security association *(Kunzinger, [0074] forwarding the IPSec datagram and [0013] and [0068] the hash value and id and address are in the packet of data) .*

Kunzinger does not expressly teach means for directly negotiating and exchanging keys, according to a key exchange protocol, between the first computer and the second computer to establish a security association having a source address of the first computer as a first end point and a destination address of the second computer as

a second end point and the intermediate computer forwarding without decrypting the secure message.

However Gunter teaches means for directly negotiating and exchanging keys, according to a key exchange protocol, between the first computer and the second computer to establish a security association *(Gunter, Fig 4 and Col 6 L36-40, external client 42 and internal client 44 establish a secure connection via the intermediate firewall using a key exchange protocol)* having a source address of the first computer as a first end point and a destination address of the second computer as a second end point *(Gunter, Fig 4, the external client 42 is the source of the secure connection and the internal client 44 is the destination)* and the intermediate computer forwarding without decrypting the secure message *(Gunter, Fig 4 #220-#224, the intermediate firewall transmits the packet without first decrypting it)*

It would have been obvious to one of ordinary skill in the art at the time of invention to combine the teachings of Kunzinger and Gunter to have the endpoints directly negotiate a key to establish a secure connection, because Gunter teaches that direct key negotiation is a well know method for two endpoints to communicate securely with an intermediary involved (Gunter Col 3 L50-57).

As to claim 23, Kunzinger and Gunter teaches wherein the translation table for IPSec translation has IP addresses of the intermediate computer to be matched with IP addresses of the second computer *(Kunzinger [0074] the gateway uses tables and id to*

translate the packet into a corresponding tunnel and the data is then forwarded/send the over the second tunnel and [0013] the new packet has the address of the second computer).

As to claim 24, Kunzinger and Gunter teaches wherein the translation tables for IKE translation consists of two partitions, one for the communication between the first computer and the intermediate computer and another for the communication between the intermediate computer and the second computer *(Kunzinger, [0066] L1-10, each set of interfaces has its own databases).*

As to claim 25, Kunzinger and Gunter teaches wherein both partitions of the mapping table for IKE translation contains translation fields for a source IP address, a destination IP address *(Kunzinger, [0067] IKE tables have the addresses for endpoint association*), initiator and responder cookies between respective computers *(Kunzinger, [0067], IDci and IDcr values).*

As to claim 26, Kunzinger and Gunter teaches wherein there is another translation table for IKE translation containing fields for matching a given user to a given computer *(Kunzinger, [0066], association for a user to an endpoint).*

As to claim 27, Kunzinger teaches a telecommunication network for secure forwarding of messages *(Kunzinger, [0047] L1-13, end to end data sending via an intermediate gateway using secure tunnels),* comprising:

a first computer, a second computer, an intermediate computer electronically connected to the first computer and the second computer *(Kunzinger, [0047] L1-13 and Fig 4, the endpoints and intermediate computer).*

means for directly negotiating and exchanging keys between the first computer and the second computer to establish a secure connection having a source address of the first computer as a first end point and a destination address of the second computer as a second end point *(Kunzinger, [0072] the cascade enabled flag can not be set and prior art negotiatiion of keys directly takes place [0007] L1-9 and [0014] L1-2 and [0017] L1-3)),* and

the intermediate computer having means for performing translation between destination addresses and secure identities *(Kunzinger [0074] the gateway uses tables and id to translate the packet into a corresponding tunnel and the data is then forwarded/send the over the second tunnel and [0013] the new packet has the address of the second computer)* for forwarding a secure message containing a unique identity received from the first computer and using the second computer in the secure connection to the second computer in the secure connection *(Kunzinger, [0074] forwarding the IPSec datagram and [0013] and [0068] the id and address are in the packet of data).*

Kunzinger does not expressly teach means for directly negotiating and exchanging keys between the first computer and the second computer to establish a secure connection having a source address of the first computer as a first end point

and a destination address of the second computer as a second end point the intermediate computer forwards without decrypting the secure message and being aware of the keys to encrypt and/or authenticate the secure message and without establishing a new secure connection.

Gunter teaches means for directly negotiating and exchanging keys between the first computer and the second computer to establish a secure connection *(Gunter, Fig 4 and Col 6 L36-40, external client 42 and internal client 44 establish a secure connection via the intermediate firewall using a key exchange protocol)* having a source address of the first computer as a first end point and a destination address of the second computer as a second end point *(Gunter, Fig 4, the external client 42 is the source of the secure connection and the internal client 44 is the destination)* the intermediate computer forwards without decrypting the secure message and being aware of the keys to encrypt and/or authenticate the secure message and without establishing a new secure connection *(Gunter, Fig 4 #220-#224, the intermediate firewall transmits the packet without first decrypting it)*

As to claim 28, Kunzinger and Gunter teaches the method further comprises the intermediate computer substituting the first unique identity with the second unique identity of the secure connection without establishing a new secure connection and without involving the second computer *(Kunzinger [0074] the gateway uses tables and id to translate the packet into a corresponding tunnel (IKE/IPSec) and the data is then*

forwarded/send the over the second tunnel and [0013] the new packet has the address of the second computer. The second computer is uninvolved in this step and no new connections are created).

As to claim 29, Kunzinger and Gunter teaches the packets between the first computer and the intermediate computers are sent using a UDP protocol *(Kunzinger [0043], the packets are UDP packets sent over the protocol)*.

6. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kunzinger and Gunter as applied to claim 1 above, and further in view of Patel (Pub No: 2002/0004900).

As to claim 3, Kunzinger and Gunter teaches the limitations of claim 1. Kunzinger and Gunter does not teach wherein the method further comprises performing a secure forwarding of the message by making use of SSL or TLS protocols. Patel teaches wherein the method further comprises performing a secure forwarding of the message by making use of SSL or TLS protocols *(Patel, [0037] L18-21, SSL for secure connection)*. It would have been obvious to one of ordinary skill in the art at the time of invention to combine the teachings of Kunzinger and Gunter with Patel to use SSL for the secure connection because Patel teaches that SSL is a well know protocol for a secure connection that can be used like IPSec.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to AFSHAWN TOWFIGHI whose telephone number is (571)270-7296. The examiner can normally be reached on Monday - Friday 9:00 A.M. to 6:00 P.M..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ian Moore can be reached on (571)272-3085. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/A. T./
Examiner, Art Unit 2469

/Ian N. Moore/
Supervisory Patent Examiner, Art Unit 2469